WHAT IS CLAIMED IS:

1. A method for providing one or more independent auditors an audit trail having one or more records for a database system, an integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditors, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditors, each record having a corresponding authentication token and a validation token, the method comprising:

initiating the audit trail by generating an initial value of an authentication token and an initial value of a validation token based on a first encryption key of a first type (writer public key) generated by the writer and a second encryption key of the first type generated by each Auditor (auditor public key);

generating a third encryption key of a second type (writer private key) related to the first encryption key and a fourth encryption key of a second type (auditor private key) related to the second encryption key;

updating the values of the writer private key, the authentication token, and the validation token while integrating the values of the validation token and the writer public key into each corresponding record of the audit trail; and

validating, by the auditor, each record of the audit trail by comparing the integrated validation token with a newly computed validation token in order to detect a tampering of the audit trail.

2. The method of claim 1 wherein the step of initiating further includes storing the initial values of the validation token and the writer public key in an initial record of the audit trail.

3. The method of claim 1 wherein the step of initiating further includes:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key;

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

4. The method of claim 1 wherein the step of generating further includes:

storing the auditor private key in a first secured storage accessible only by the auditor; and

storing the writer private key in a second secured storage accessible only by the writer.

5. The method of claim 1 wherein the step of updating further includes:

updating the value of the writer private key;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key and the auditor public key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

6. The method of claim 1 wherein the newly computed validation token is generated by the auditor based on the auditor private key and the writer public key.

7. A method for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database system, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditor, the method comprising:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

8. The method of claim 7 wherein the step of integrating further includes:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

9. The method of claim 8 wherein the step of initiating further includes:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

10. The method of claim 9 wherein the step of initiating further includes:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the stored auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the auditor to compute the values of the validation token for the records to verify against the integrated values of the validation token.

11. The method of claim 8 wherein the step of updating further includes:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

12. A computer program for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database system, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database system having a writing machine (writer) not under the control of the access-privileged user or the auditor, the computer program comprising instructions for:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

13. The computer program of claim 12 wherein the means for integrating further includes instructions for:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

14. The computer program of claim 13 wherein the means for initiating further includes instructions for:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

15. The computer program of claim 14 wherein the means for initiating further includes instructions for:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the auditor to compute the values of the validation token for the records to verify against the integrated values of the validation token.

16. The computer program of claim 13 wherein the means for updating further includes instructions for:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.

17. A system for providing at least one independent auditor an audit trail, the audit trail having one or more records recording actions taken against a database, the integrity of the audit trail being vulnerable to actions taken by an access-privileged user other than the auditor, the database having a writing machine (writer) not under the control of the access-privileged user or the auditor, the system comprising means for:

integrating into each record a corresponding value of a validation token generated based on a first pair of public-private encryption keys generated by the writer and a second pair of public-private encryption keys generated by the auditor,

wherein the writer has an access to the public encryption key of the second pair (auditor public key), and the auditor has an access to the public encryption key of the first pair (writer public key),

wherein only the writer has an access to the private key of the first pair (writer private key), and only the auditor has an access to the private key of the second pair (auditor private key), and

wherein the auditor has the ability to compute the values of the validation token for the records to verify against the integrated values of the validation token in order to detect a tampering of the audit trail by the access-privileged user.

18. The system of claim 17 wherein the means for integrating further includes means for:

initiating the audit trail by generating an initial value of the authentication token and an initial value of the validation token for an initial record of the audit trail based on the writer public key and the auditor public key; and

updating the values of the writer private key, the authentication token, and the validation token,

wherein each updated value of the validation token is integrated into a corresponding record of the audit trail.

19. The system of claim 18 wherein the means for initiating further includes means for:

concatenating a predetermined identity for the audit trail, and a common initialization encryption key generated by the auditor with the auditor public key and the writer public key; and

generating the initial value of the validation token through at least one hashing process and at least one encryption process using the concatenated result,

wherein the initial value of the authentication token is used as an encryption key for the encryption process.

20. The system of claim 19 wherein the means for initiating further includes means for:

storing the auditor private key, the identity for the audit trail, and the initial record in a designated secured information storage accessible only by the auditor,

wherein the stored auditor private key, the identity for the audit trail, and the initial record can be retrieved by the auditor and used with the writer public key accessible by the auditor to compute the values of the validation token for the records to verify against the integrated values of the validation token.

21. The system of claim 18 wherein the means for updating further includes means for:

updating the value of the writer private key through a hashing process;

updating the value of the writer public key based on the updated writer private key;

updating the value of the authentication token by a hashing process based on the updated value of the writer private key; and

updating the value of the validation token through at least a hashing process and an encryption process,

wherein the updated authentication token is used as an encryption key for the encryption process while updating the value of the validation token.